APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,212	03/30/2004	Iyad Qumei	15619US02	4068

23446 7590 06/23/2008	EXAMINER
MCANDREWS HELD & MALLOY, LTD	CHEN, SHIN HON
500 WEST MADISON STREET	
SUITE 3400	
CHICAGO, IL 60661	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/813,212
Filing Date: March 30, 2004
Appellant(s): QUMEI, IYAD

Kevin E. Borg
Reg. No. 51,486
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/3/08 appealing from the Office action

mailed 11/23/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 1, 2, 4-12, 22-28, 30-38 and 41 are rejected.

Claims 13-21 are allowed.

Claims 3, 29, 39 and 40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 1, 2, 4-9, 12, 22-28, 30, 31 and 41 stand rejected under 35 U.S.C 102(a) as being anticipated by U.S. Pub. No. 2003/0051160 (Selkirk).

Claims 10, 11 and 32-38 stand rejected under 35 U.S.C 103(a) as being unpatentable over Selkirk in view of U.S. Pat. No. 6,230,316 (Nachenberg).

Rejection to claim 3 under 35 U.S.C 102(a) as being anticipated by U.S. Pub. No. 2003/0051160 (Selkirk) has been withdrawn.

Rejection to claims 13-21, 29, 39 and 40 under 35 U.S.C 103(a) as being unpatentable over Selkirk in view of U.S. Pat. No. 6,230,316 (Nachenberg) has been withdrawn.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. Rejection to claims 3, 13-21, 29, 39 and 40 are withdrawn by the examiner as claims 13-21 are allowed and claims 3, 29, 39 and 40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 3, the prior of record discloses transmitting encrypted firmware update from server to firmware device and the firmware device decrypts the firmware updates for storage. However, the prior art of record does not explicitly disclose wherein at least a portion of the at least one of firmware and software **resident** in the electronic device is encrypted.

Regarding claim 13-21, the prior art of record discloses generating encrypted firmware update. However, the prior art of record individually or in combination does not explicitly disclose generating binary difference information using a first firmware image and a second firmware image, wherein one or both of the first and second firmware images are partially or entirely encrypted, and wherein generating comprises decrypting encrypted portions of the first and second firmware images.

Regarding claim 29, the prior art of record discloses updating the firmware update in the firmware device by decrypting the encrypted firmware update. However, the prior art of record individually or in combination does not explicitly disclose wherein at least a portion of the at least one of firmware and software application resident in the electronic device is encrypted and stored in one of an encrypted data section and an encrypted code section.

Regarding claims 39 and 40, the prior art of record disclose decrypting encrypted firmware update by the firmware device. However, the prior art of record does not explicitly disclose decrypting an original data block and copying the decrypted data block to random access memory; applying update information to the random access memory, the update information comprising at least one of an update code and an update data segment from a data update package; updating the decrypted data block with the update information to form an updated decrypted data block; and encrypting the updated decrypted data block to from an encrypted updated data block.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0051160	SELKIRK	3-2003
6,230,316	NACHENBERG	5-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2.   Claims 1, 2, 4-9, 12, 22-28, 30, 31 and 41 are rejected under 35 U.S.C. 102(a) as

being anticipated by Selkirk et al. U.S. Pub. No. 20030051160 (hereinafter Selkirk).

3.   As per claim 1, Selkirk discloses an electronic device network for updating at

least one of firmware and software in a plurality of electronic devices using at least one

electronic device update, the network comprising: at least one update generator adapted

to generate updates, the at least one update generator comprising an encrypting and

decrypting engine (Selkirk: [0017]: server generated updates and transmits updates

securely to firmware); at least one update store storing a plurality of electronic device

updates (Selkirk: [0017]: update server); and at least one update delivery server adapted

to dispense the plurality of electronic device updates (Selkirk: [0017]: server downloads

update to firmware device); and wherein at least one of the firmware and software in the

plurality of electronic devices and the at least one update being encrypted (Selkirk:

[0009] and [0017]: the firmware updates are encrypted so that only firmware can decrypt the updates).

4.   As per claim 2, Selkirk discloses the network of claim 1. Selkirk further discloses wherein the at least one update delivery server comprises secure socket layer support providing authentication and data encryption/decryption (Selkirk: [0017]: updates being provided through SSL).

5.   As per claim 4, Selkirk discloses the network of claim 1. Selkirk further discloses wherein each of the plurality of electronic devices comprises: one of encrypting and decrypting components; and a client for downloading updates (Selkirk: [0017]: the firmware device supports cryptographic functions).

6.   As per claim 5, Selkirk discloses the network of claim 1. Selkirk further discloses wherein each of the plurality of electronic devices comprises a security services component providing secure communication with the at least one update delivery server (Selkirk: [0017]).

7.   As per claim 6, Selkirk discloses the network of claim 1. Selkirk further discloses wherein each of the plurality of electronic devices comprises an encrypted section, the encrypted section comprising at least one of an encrypted data section and an encrypted code section (Selkirk: [0017]).

8.   As per claim 7, Selkirk discloses the network of claim 1. Selkirk further discloses

wherein each of the plurality of electronic devices comprises an encrypted section, the

encrypted section comprising at least one of an encrypted data section and an encrypted

code section (Selkirk: [0008]: firmware comprises data and code).

9.   As per claim 8, Selkirk discloses the network of claim 7. Selkirk further discloses

wherein the update agent is adapted to employ at least one of encrypting and decrypting

components to update at least one of firmware and software resident in the electronic

devices, and wherein at least a portion of the at least one of firmware and software is

encrypted and stored in one of an encrypted data section and an encrypted code section

(Selkirk: [0008]: firmware contains data and code; [0017]: encrypted firmware).

10.   As per claim 9, Selkirk discloses the network of claim 1. Selkirk further discloses

wherein the update generator is adapted to process an old memory image and a new

image of the at least one of firmware and software in the electronic devices, and wherein

at least a portion of the at least one of firmware and software is encrypted (Selkirk:

[0017]).

11.   As per claim 12, Selkirk discloses the network of claim 1. Selkirk further

discloses wherein the electronic devices comprise a plurality of mobile electronic

devices, and wherein the plurality of mobile electronic devices comprise at least one of a

mobile cellular phone handset, personal digital assistant, pager, a multimedia player, and

a camera (Selkirk: [0021]: pda).

12.   As per claim 22-28 and 30 encompass the same scope as claims 1, 2, 4-9 and 12.

Therefore, claims 22-28 are rejected based on the same reason set forth above in rejecting

claims 1, 2, 4-9 and 12.

13.   As per claim 31, Selkirk discloses a method of building a firmware upgrade for

use in an electronic device incorporating encryption, the method comprising: building a

firmware image to be encrypted (Selkirk: [0017]: the firmware device requests firmware

update from server and the server encrypts the firmware image and transmits the data to

the firmware device), the firmware image comprising a plurality of components; and

encrypting the components before assembling the component's into an encrypted

firmware image (Selkirk: [0034]: encryption utilizes RC4/symmetric stream cipher that

performs encryption using keystream through bit-wise operation so that components of

firmware update encrypted before assembly).

14.   As per claim 41, Selkirk discloses the method according to claim 31. Selkirk

further discloses wherein the electronic devices comprise a plurality of mobile electronic

devices, and wherein the plurality of mobile electronic devices comprise at least one of a

mobile cellular phone handset, personal digital assistant, pager, a multimedia player, and

a camera (Selkirk: [0021]: PDA).

Claim Rejections - 35 USC § 103

15.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

16.   Claims 10, 11 and 32-38 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Selkirk in view of Nachenberg U.S. Pat. No. 6230316 (hereinafter

Nachenberg).

17.   As per claim 10, Selkirk discloses the network of claim 1. Selkirk discloses

firmware updates (Selkirk: [0017]). Selkirk does not explicitly disclose wherein the

update generator is adapted to decipher one of encrypted data segments and encrypted

code in both an old memory image and a new image to generate an update for updating at

least one of firmware and software in the electronic devices. However, Nachenberg

discloses generating an update file by performing binary difference between old file and

new file (Nachenberg: column 5 lines 37-50). It would have been obvious to one having

ordinary skill in the art to generate a firmware update by binary differencing the new and

old image because binary difference is well known technique for update. Therefore, it

would have been obvious to one having ordinary skill in the art at the time of applicant's

invention to combine the teachings of Nachenberg within the system of Selkirk because

incremental update of a file provides efficient update process.

18.   As per claim 11, Selkirk discloses the network of claim 1. Selkirk does not

explicitly disclose wherein the update generator is adapted to employ deciphering

techniques to extract one of ciphered code and enciphered data segments, process the one

of enciphered code and enciphered data segments to generate an update comprising

difference information, and cipher the one of code and data segments, and the difference

information in at least one update. However, Nachenberg discloses generating an update

file by performing binary difference between old file and new file (Nachenberg: column

5 lines 37-50). It would have been obvious to one having ordinary skill in the art to

generate a firmware update by binary differencing the new and old image because binary

difference is well known technique for update. Therefore, it would have been obvious to

one having ordinary skill in the art at the time of applicant's invention to combine the

teachings of Nachenberg within the system of Selkirk because incremental update of a

file provides efficient update process.

19.   As per claim 32, Selkirk discloses the method of claim 31. Selkirk does not

explicitly disclose the limitation of claim 32. However, Nachenberg discloses generating

binary difference information between firmware versions undergoing an upgrade; and

using an un-encrypted firmware image to generate the binary difference information,

wherein as the upgrade is being applied to an encrypted firmware image, uncorrelated

information is decrypted (Nachenberg: column 5 lines 37-50). It would have been

obvious to one having ordinary skill in the art to generate a firmware update by binary

differencing the new and old image because binary difference is well known technique

for update. Therefore, it would have been obvious to one having ordinary skill in the art

at the time of applicant's invention to combine the teachings of Nachenberg within the system of Selkirk because incremental update of a file provides efficient update process.

20.   As per claim 33, Selkirk as modified discloses the method of claim 31. Selkirk as modified further discloses creating a data update package, the data update package being based upon un-encrypted binary images (Nachenberg: column 5 lines 37-50).

21.   As per claim 34, Selkirk as modified discloses the method of claim 31. Selkirk as modified further discloses creating a data update package, the data update package being based upon encrypted binary images (Selkirk: [0017]).

22.   As per claim 35-38, Selkirk as modified discloses the method of claim 31. Selkirk as modified does not explicitly disclose pre-check analysis, check-recovery analysis, and fault tolerant procedures. However, Selkirk disclosed that the upgrade data transmitted from server to firmware device is encrypted and protected and one with ordinary skill in the art would understand using Cyclic Redundancy Check or other well-known message authentication code to verify the integrity of the data is intact and ensure that the data is not subject to tampering. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to utilize pre-check analysis, check-recovery analysis and fault tolerant procedures to ensure that integrity of encrypted data transmitted from server to client is not compromised because these procedures are well known in the art to verify data integrity for secure data communication.

(10) Response to Argument

I.   Selkirk Does Not Anticipate Claims 1-9 and 12.

Regarding appellant's argument on claims 1-9 and 12, appellant argues that the
prior art of record does not explicitly disclose "wherein at least a portion of the at least
one of firmware and software in the plurality of electronic devices is encrypted".
However, the examiner disagrees. The examiner has relied on the Selkirk reference to
disclose securely transmitting encrypted firmware update from server to client and no
decryption of the encrypted firmware update takes place outside of the firmware device
(Selkirk: [0017] lines 18-25: the firmware update is a portion of the firmware and
software of the electronic device). Therefore, when the firmware device receives
firmware update/portion of the firmware and software in the electronic device, the
firmware update is in encrypted state prior to decryption.

On the other hand, appellant argues that the Selkirk reference does not
disclose "updating encrypted firmware or software". However, claim 1 does not recite the
limitation "updating encrypted firmware of software". Therefore, examiner is not
required to consider such limitation. In response to applicant's argument that the
references fail to show certain features of applicant's invention, it is noted that the
features upon which applicant relies (i.e., "updating encrypted firmware or software") are
not recited in the rejected claim(s). Although the claims are interpreted in light of the
specification, limitations from the specification are not read into the claims. See *In re
Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Furthermore, appellant argues that the Selkirk reference fails to mention anything
about generating an update. However, the examiner disagrees. Selkirk discloses that a

client/firmware device requests firmware update from a server and the server generates

encrypted firmware update and provides it to the firmware device (Selkirk: [0017] lines

7-10 and 17-22). Therefore, although Selkirk does not disclose in detail generation of the

update, paragraph [0017] provides sufficient information pertaining to generation of

firmware update as coming from the server which implies that the server is responsible

for generation of the update.

II.   The Proposed Combination of Selkirk and Nachenberg Does Not Render
Claims 10, 11 and 34-41 Unpatentable.

A.   The Proposed Combination Does Not Render Claims 13-21
Unpatentable.

Appellant's argument regarding claims 13-21 are persuasive. Therefore, rejection

of claim 13-21 has been withdrawn.

B.   The Proposed Combination Does Not Render Claims 22-30
Unpatentable.

Regarding claims 22-30, appellant mainly argues that the Selkirk reference does

not disclose a first-in-first-out (FIFO) memory device. However, the examiner disagrees.

Selkirk discloses the firmware memory is connected to internal bus and provides storage

for the actual firmware and is preferably some kind of write-able non-volatile memory

such as EEPROM, flash ROM and non-volatile RAM (Selkirk: [0024]). Therefore,

although no specific word mentions "FIFO" and FIFO memory does not appears to be a

patentable feature, the memory device disclosed by Selkirk discloses the hardware

limitation disclosed by appellant. In addition, the claim only recites of a FIFO memory

device but fails to distinguish how the FIFO is used in relation to updating of firmware.

       C.   **The Proposed Combination Does Not Render Claims 31-41**

Unpatentable.

      Regarding claims 31, appellant mainly argues that the Selkirk reference does not

disclose "encrypting the components before assembling the components into an

encrypted firmware image". However, the examiner disagrees. Selkirk discloses that

firmware update is subject to encryption and the encryption preferably uses RC4

cipher/stream cipher or DES/block cipher that encrypts data by performing encryption

block by block/component by component (Selkirk: [0034]). Therefore, the components of

firmware update are encrypted prior to being assembled into an update packet.

       D.   **The Proposed Combination Does Not Render Claim 36 Unpatentable.**

      Regarding claim 36, appellant argues that the prior art of record does not disclose

pre-check analysis, check recover analysis. However, the examiner has indicated that the

Selkirk discloses protecting the firmware update from unauthorized tampering and

access. Although the prior art of record does not explicitly disclose the procedures

disclosed in claim 36, the procedures disclosed in claim 36 are well known in the art to

provide data integrity check that ensures data has not been illicitly modified/tampered.

Therefore, it would have been obvious to one having ordinary skill in the art to combine

the data integrity check procedures to the teachings of Selkirk to protect data from

unauthorized modification because data privacy, integrity and authenticity are key features of secure data communication.

E.   The Proposed Combination Does Not Render Claim 37 Unpatentable.

Regarding claim 37, appellant argues that the prior art of record does not disclose "a cyclic redundancy check" (CRC). However, the examiner has indicated that it would have been obvious to one having ordinary skill in the art to verify the integrity of data after secure data communication to ensure that the data has not been tampered or modified. To ensure data integrity, cyclic redundancy check and message authentication are most often used as well known in the art. Therefore, although the prior art of record does not explicitly disclose the use of CRC, the use of CRC is well known in the art and does not appear to be patentable.

F.   The Proposed Combination Does Not Render Claim 40 Unpatentable.

Regarding claim 40, appellant's argument is persuasive. Therefore, rejection to claim 40 has been withdrawn.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Shin-Hon Chen

/Shin-Hon Chen/

Primary Examiner, Art Unit 2131

Conferees:

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2131

Ayaz Sheikh

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131